

In re the Application of

Inventors: Takeshi TANAKA, et al.

Application No.: New PCT National Stage Application

Filed: April 21, 2005

For: RADIO COMMUNICATION MANAGEMENT METHOD AND RADIO
COMMUNICATION MANAGEMENT SERVER

CLAIM FOR PRIORITY

Assistant Commissioner of Patents
Washington, D.C. 20231

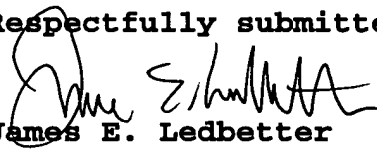
Dear Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified application and the priority provided in 35 USC 119 is hereby claimed:

Japanese Appln. No. 2002-311910, filed October 25, 2002.

It is requested that the file of this application be marked to indicate that the requirements of 35 USC 119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,


James E. Ledbetter
Registration No. 28,732

Date: April 21, 2005

JEL/ejw
Attorney Docket No. L8638.05102
STEVENS DAVIS, MILLER & MOSHER, L.L.P.
1615 L STREET, NW, Suite 850
P.O. Box 34387
WASHINGTON, DC 20043-4387
Telephone: (202) 785-0100
Facsimile: (202) 408-5200

PCT/JP 03/13624

日 本 国 特 許 庁
JAPAN PATENT OFFICE

24.10.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 2 年 1 0 月 2 5 日

出 願 番 号
Application Number: 特 願 2 0 0 2 - 3 1 1 9 1 0
[ST. 10/C]: [J P 2 0 0 2 - 3 1 1 9 1 0]

出 願 人
Applicant(s): 松下電器産業株式会社

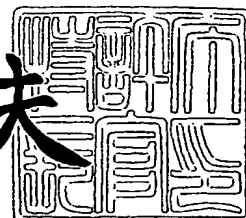
RECEIVED	
12 DEC 2003	
WIPO	PCT

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2 0 0 3 年 1 1 月 2 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 9 7 9 3 6

【書類名】 特許願
【整理番号】 2900645253
【あて先】 特許庁長官殿
【国際特許分類】 H04L 12/46
H04L 12/28
G06F 13/00
H04L 12/66

【発明者】

【住所又は居所】 神奈川県横浜市港北区綱島東四丁目 3 番 1 号 松下通信
工業株式会社内

【氏名】 田中 武志

【発明者】

【住所又は居所】 神奈川県横浜市港北区綱島東四丁目 3 番 1 号 松下通信
工業株式会社内

【氏名】 青山 高久

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100093067

【弁理士】

【氏名又は名称】 二瓶 正敬

【手数料の表示】

【予納台帳番号】 039103

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0003222

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 無線通信管理及び無線通信管理サーバ

【特許請求の範囲】

【請求項 1】 H M I P v 6 を用いて移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法であって、

前記移動端末の前記リンク接続を管理するサーバに対して、前記移動端末が、前記リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、前記移動端末の前記リンク接続の変更に要する時間を短縮する無線通信管理方法。

【請求項 2】 前記移動端末が、前記リンク接続を変更するための情報と、前記認証に係る情報とを 1 つの情報として送信し、前記リンク接続を管理するサーバが、前記 1 つの情報から、前記リンク接続を変更するための情報及び前記認証に係る情報のそれぞれを取得する請求項 1 に記載の無線通信管理方法。

【請求項 3】 前記リンク接続を管理するサーバが、前記認証に係る情報を用いた認証処理による認証結果を取得する請求項 1 又は 2 に記載の無線通信管理方法。

【請求項 4】 前記リンク接続を管理するサーバが、前記移動端末の認証を行う認証サーバとの通信を行い、前記認証結果を取得する請求項 3 に記載の無線通信管理方法。

【請求項 5】 前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と、前記認証結果とを 1 つの情報として、前記移動端末に送信する請求項 3 又は 4 に記載の無線通信管理方法。

【請求項 6】 前記リンク接続を管理するサーバが、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報を前記移動端末に送信し、その後、前記認証結果を取得できた場合に前記認証結果を前記移動端末に送信する請求項 3 から 5 のいずれか 1 つに記載の無線通信管理方法。

【請求項 7】 前記リンク接続を管理するサーバが、前記認証結果の取得までの時間を設定し、前記認証結果の取得までの時間内に前記認証結果を取得できた場合、次に前記移動端末から前記リンク接続を変更するための情報を受信した際

に、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、前記認証結果を前記移動端末に送信する請求項 6 に記載の無線通信管理方法。

【請求項 8】 前記リンク接続を管理するサーバが、前記移動端末が前記所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定し、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、前記所定の時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信する請求項 7 に記載の無線通信管理方法。

【請求項 9】 前記リンク接続を管理するサーバが、前記所定の仮許可時間よりも長い時間であって、前記移動端末が前記所望のネットワークへのアクセスを許可する所定の許可時間を設定し、前記認証結果が認証成功であった場合、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、所定の許可時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信する請求項 5 から 8 のいずれか 1 つに記載の無線通信管理方法。

【請求項 10】 前記リンク接続を管理するサーバが、前記所定の仮許可時間又は前記所定の許可時間だけ前記所望のネットワークへのアクセスを許可した前記移動端末の前記リンク接続の変更に係る登録を行い、前記所定の仮許可時間又は前記所定の許可時間が経過した場合、前記移動端末の前記リンク接続の変更に係る登録を削除する請求項 8 又は 9 に記載の無線通信管理方法。

【請求項 11】 前記リンク接続を管理するサーバが、前記認証結果の取得までの時間を設定し、前記認証結果の取得までの時間内に前記認証結果を取得できなかった場合、前記認証結果を認証失敗とする請求項 3 から 5 のいずれか 1 つに記載の無線通信管理方法。

【請求項 12】 前記リンク接続を管理するサーバが、前記移動端末に対して所定の接続禁止時間を設定し、前記移動端末に対して前記認証結果として認証失敗を通知した場合には、前記認証失敗の通知から前記所定の接続禁止時間だけ、前記認証失敗であった前記移動端末の前記リンク接続の変更に係る処理及び前記認証に係る処理を行わないようにする請求項 5 から 11 のいずれか 1 つに記載の無線通信管理方法。

【請求項 13】 前記リンク接続を管理するサーバが、前記移動端末に対して

前記認証結果として認証成功を通知した場合のみ、前記認証成功であった前記移動端末の前記リンク接続の変更に係る登録を行うようにする請求項 5 から 10 のいずれか 1 つに記載の無線通信管理方法。

【請求項 14】 移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法であって、

前記移動端末の前記リンク接続を管理するサーバに対して、前記移動端末が、前記リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、

前記リンク接続を管理するサーバが、前記認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定し、前記認証結果の取得までの時間内に前記認証結果を取得できた場合、前記認証結果を前記移動端末に送信する無線通信管理方法。

【請求項 15】 前記リンク接続を管理するサーバが、前記移動端末が前記所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定し、前記所定の時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信する請求項 14 に記載の無線通信管理方法。

【請求項 16】 前記リンク接続を管理するサーバが、前記所定の仮許可時間よりも長い時間であって、前記移動端末が前記所望のネットワークへのアクセスを許可する所定の許可時間を設定し、前記認証結果が認証成功であった場合、所定の許可時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信する請求項 15 に記載の無線通信管理方法。

【請求項 17】 前記所定の仮許可時間又は前記所定の許可時間が経過した場合、前記リンク接続を管理するサーバは、前記移動端末の前記接続を切断する請求項 15 又は 16 に記載の無線通信管理方法。

【請求項 18】 移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法であって、

前記移動端末の前記リンク接続を管理するサーバに対して、前記移動端末が、前記リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、

前記リンク接続を管理するサーバが、前記認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定し、前記認証結果の取得までの時間内に前記認証結果を取得できなかった場合、前記認証結果を認証失敗とする無線通信管理方法。

【請求項 1 9】 前記リンク接続を管理するサーバが、前記移動端末に対して所定の接続禁止時間を設定し、前記移動端末に対して前記認証結果として認証失敗を通知した場合には、前記認証失敗の通知から前記所定の接続禁止時間だけ、前記認証失敗であった前記移動端末に係る処理を行わないようにする請求項 1 4 から 1 8 のいずれか 1 つに記載の無線通信管理方法。

【請求項 2 0】 前記リンク接続を管理するサーバが、前記移動端末に対して前記認証結果として認証成功を通知した場合のみ、前記認証成功であった前記移動端末の前記リンク接続の変更に係る登録を行うようにする請求項 1 4 から 1 7 のいずれか 1 つに記載の無線通信管理方法。

【請求項 2 1】 H M I P v 6 を用いて移動端末のリンク接続を管理する無線通信管理サーバであって、

前記移動端末から、前記リンク接続を変更するための情報と所望のネットワークにアクセスするための認証に係る情報とを 1 つの情報で受信し、前記 1 つの情報から、前記リンク接続を変更するための情報及び前記認証に係る情報のそれぞれを取得するよう構成されている無線通信管理サーバ。

【請求項 2 2】 前記認証に係る情報を用いた認証処理による認証結果を取得するよう構成されている請求項 2 1 に記載の無線通信管理サーバ。

【請求項 2 3】 前記移動端末の認証を行う認証サーバとの通信を行う手段を有し、

前記認証結果を取得するよう構成されている請求項 2 2 に記載の無線通信管理サーバ。

【請求項 2 4】 前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と前記認証結果とを 1 つの情報として、前記移動端末に送信するよう構成されている請求項 2 2 又は 2 3 に記載の無線通信管理サーバ。

【請求項 2 5】 前記移動端末の前記リンク接続の変更を確認した旨を通知す

る情報を前記移動端末に送信し、その後、前記認証結果を取得できた場合に前記認証結果を前記移動端末に送信するよう構成されている請求項 22 から 24 のいずれか 1 つに記載の無線通信管理サーバ。

【請求項 26】 前記認証結果の取得までの時間を設定する時間設定手段を有し、前記認証結果の取得までの時間内に前記認証結果を取得できた場合、次に前記移動端末から前記リンク接続を変更するための情報を受信した際に、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、前記認証結果を前記移動端末に送信するよう構成されている請求項 25 に記載の無線通信管理サーバ。

【請求項 27】 前記移動端末に対して前記所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定する時間設定手段を有し、

前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、前記所定の時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信するよう構成されている請求項 26 に記載の無線通信管理サーバ。

【請求項 28】 前記移動端末に対して、前記所定の仮許可時間よりも長い時間であって、前記移動端末が前記所望のネットワークへのアクセスを許可する所定の許可時間を設定する時間設定手段を有し、

前記認証結果が認証成功であった場合、前記移動端末の前記リンク接続の変更を確認した旨を通知する情報と共に、所定の許可時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信するよう構成されている請求項 24 から 27 のいずれか 1 つに記載の無線通信管理サーバ。

【請求項 29】 前記所定の仮許可時間又は前記所定の許可時間だけ前記所望のネットワークへのアクセスを許可した前記移動端末の前記リンク接続の変更に係る登録を行う情報登録手段と、

前記所定の仮許可時間又は前記所定の許可時間が経過した場合、前記移動端末の前記リンク接続の変更に係る登録を削除する情報削除手段とを、

有する請求項 27 又は 28 に記載の無線通信管理サーバ。

【請求項 30】 前記認証結果の取得までの時間を設定する時間設定手段と、

前記認証結果の取得までの時間内に前記認証結果を取得できなかった場合、前記認証結果を認証失敗とする判定手段とを、

有する請求項 22 から 24 のいずれか 1 つに記載の無線通信管理サーバ。

【請求項 31】 前記移動端末に対して所定の接続禁止時間を設定する時間設定手段と、

前記移動端末に対して前記認証結果として認証失敗を通知した場合には、前記認証失敗の通知から前記所定の接続禁止時間だけ、前記認証失敗であった前記移動端末の前記リンク接続の変更に係る処理及び前記認証に係る処理を行わないよう制御する制御手段とを、

有する請求項 24 から 30 のいずれか 1 つに記載の無線通信管理サーバ。

【請求項 32】 前記移動端末に対して前記認証結果として認証成功を通知した場合のみ、前記認証成功であった前記移動端末の前記リンク接続の変更に係る登録を行うよう制御する制御手段を有する請求項 24 から 29 のいずれか 1 つに記載の無線通信管理サーバ。

【請求項 33】 移動端末のリンク接続を管理する無線通信管理サーバであって、

前記移動端末から、前記リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を受信する受信手段と、

前記認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定する時間設定手段と、

前記認証結果の取得までの時間内に前記認証結果を取得できた場合、前記認証結果を前記移動端末に送信する送信手段とを、

有する無線通信管理サーバ。

【請求項 34】 前記移動端末が前記所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定する時間設定手段を有し、

前記所定の時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信するよう構成されている請求項 33 に記載の無線通信管理サーバ。

【請求項 35】 前記所定の仮許可時間よりも長い時間であって、前記移動端

末が前記所望のネットワークへのアクセスを許可する所定の許可時間を設定する時間設定手段を有し、

前記認証結果が認証成功であった場合、所定の許可時間だけ前記所望のネットワークへのアクセスの許可を通知する情報を前記移動端末に送信するよう構成されている請求項 34 に記載の無線通信管理サーバ。

【請求項 36】 前記所定の仮許可時間又は前記所定の許可時間が経過した場合、前記移動端末の前記接続を切断する制御手段を有する請求項 34 又は 35 に記載の無線通信管理サーバ。

【請求項 37】 移動端末のリンク接続を管理する無線通信システムにおける無線通信管理サーバであって、

前記移動端末から、前記リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を受信する受信手段と、

前記リンク接続を管理するサーバが、前記認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定する時間設定手段と、

前記認証結果の取得までの時間内に前記認証結果を取得できなかった場合、前記認証結果を認証失敗として、前記認証結果を前記移動端末に送信する送信手段とを、

有する無線通信管理サーバ。

【請求項 38】 前記移動端末に対して所定の接続禁止時間を設定する時間設定手段と、

前記移動端末に対して前記認証結果として認証失敗を通知した場合には、前記認証失敗の通知から前記所定の接続禁止時間だけ、前記認証失敗であった前記移動端末に係る処理を行わないよう制御する制御手段とを、

有する請求項 33 から 37 のいずれか 1 つに記載の無線通信管理サーバ。

【請求項 39】 前記移動端末に対して前記認証結果として認証成功を通知した場合のみ、前記認証成功であった前記移動端末の前記リンク接続の変更に係る登録を行うよう制御する制御手段を有する請求項 33 から 36 のいずれか 1 つに記載の無線通信管理サーバ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、移動端末がリンク接続を変更する際に、通信が途切れないように移動端末のアドレスの変更を行う無線通信管理システム及び無線通信管理サーバに関し、特に、HMIP v 6 (Hierarchical Mobile IP version 6: 階層型モバイルIP v 6) を用いて移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法及び無線通信管理サーバに関する。

【0002】

【従来の技術】

利用者が、移動端末 (Mobile Terminal) を利用してネットワークと通信を行う場合、アクセスを提供しているオペレータは、移動端末とネットワークとの接続サービスを提供する前に、移動端末がネットワークと接続する権利を有するか否かを判定 (認証) する必要がある。この認証処理は、アクセスを提供しているオペレータの施設である中間ノードが、移動端末に対してネットワークとの接続サービスを提供する前に、移動端末からの接続要求に含まれる認証情報 (端末ID及び利用者情報の組合せ) を認証サーバに問い合わせ、認証サーバからの応答に含まれる認証結果に従って、移動端末に対するネットワークとの接続サービスを提供するか否かを判断することにより実現される。なお、必要に応じて、ネットワークを介して、利用者のオペレータの施設に存在する所定の認証サーバに対して認証を依頼することも可能である。本明細書では、このシーケンスを認証シーケンスと呼ぶことにする。

【0003】

例えば、後述の非特許文献1に記載の技術であるIEEE802.11xを無線LANに適用した場合には、移動端末が、ネットワークと接続する際の入り口となるアクセスポイント (Access Point) と接続する際にアクセスポイントに認証情報を送り、アクセスポイントが移動端末の認証サーバに対して認証要求を行うことによって認証処理の実現が可能となっている。

【0004】

ところで近年、移動端末のワイヤレス化に伴い、移動端末が利用する中間ノー

ドを連続的に切り替えて移動しながら、ネットワークとの継続的な通信を行う場合が増えている。この場合、移動端末にパケットを届けるためには、ネットワーク内のいずれかのノードが、何らかの方法で移動端末の位置を特定する機能を有する必要がある。この移動端末の位置を特定する機能を有するノードは、位置管理サーバと呼ばれ、通常、移動端末の所属する利用者のオペレータに設置される（すなわち、移動端末は、利用者のオペレータの加入者である）。

【0005】

移動端末がネットワークとの通信を継続しながら、利用する中間ノードを切り替えるシームレスハンドオーバーは、通常、ネットワーク内に設置された位置管理サーバに対して、移動端末が位置登録を行うことにより実現可能である。なお、本明細書では、このシーケンスを位置登録シーケンスと呼ぶことにする。

【0006】

なお、認証シーケンスと位置登録シーケンスとは、シーケンスに係るノードが異なっている。すなわち、認証シーケンスでは、移動端末とネットワークへのアクセスを提供しているドメイン内のサーバとの通信が行われるのに対し、位置登録シーケンスでは、移動端末とネットワーク内の位置管理サーバとの通信が行われる。

【0007】

移動端末は、認証シーケンスや位置登録シーケンスが完了するまでの間、ネットワークとの通信を行うことができないため、これらのシーケンスはできるだけ短いことが望ましい。このため、後述の非特許文献2に記載されているように、認証シーケンスと位置登録シーケンスとを組み合わせるDiameter Mobile IPv4 Applicationが考えられている。このDiameter Mobile IPv4 Applicationは、IPv4環境下でシームレスハンドオーバーを可能とする技術である後述の非特許文献3記載のMobile IPv4シーケンス中に、上記のシーケンスを含めるものである。

【0008】

図9は、従来の技術に係るDiameter Mobile IPv4 Applicationのシーケンスを示す図である。図9には、利用者がネットワーク54と接続して通信を行うために利用する移動端末51、移動端末51に対してネットワーク54へのアクセス

を提供しているオペレータ 57 内のフォーリンエージェント 52 及び認証サーバ 53、ネットワーク 54、ネットワーク 54 上に存在し、利用者の端末のアドレスを管理する利用者のオペレータ 58 内に配置されたホームエージェント 55 及び認証サーバ 56 が図示されている。

【0009】

Mobile IPv4機能を搭載した移動端末は、アクセスを提供しているオペレータ 57 内（フォーリンネットワーク）に設置された中間ノード（フォーリンエージェント 52）経由で、位置管理サーバ（ホームエージェント 55）に対して位置登録シーケンスを行う。Diameter Mobile IPv4 Applicationでは、Mobile Node が位置登録を行う際に、フォーリンエージェント 52 に対して送信する位置登録メッセージ（Binding Update）内に、移動端末 51 の認証情報が付加され、フォーリンエージェント 52 が、アクセスを提供しているオペレータ 57 内の認証サーバ 53 又は利用者のオペレータ 58 内の認証サーバ 56 に対して認証要求を行うことにより、認証シーケンスが可能となっている。

【0010】

一方、移動端末が、ネットワーク上の接続リンクを変更した場合でも、ある特定のアドレス（IP アドレス）を用いて通信することを可能とし、現在継続中の通信を中断することなくシームレスに接続リンクの変更を可能とする Mobile IPv6 技術の標準化が IETF の Mobile IP Working Group において進められている。この IPv6 環境におけるシームレスハンドオーバをサポートするプロトコルである Mobile IPv6（後述の非特許文献 4 参照）の位置登録シーケンスは、Mobile IPv4 で規定されていたフォーリンエージェント 52 のような『アクセスを提供しているオペレータ 57 内の中間ノード』を経由せずに行われる。

【0011】

Mobile IPv6 では、基本的に下記の 1～3 の動作によって、移動端末がアクセスリンク（アクセスネットワーク）に接続中も、ホームアドレス宛てのパケットを受け取ることが可能となる。

【0012】

1. Care-of Address の取得

Mobile Nodeは、接続するリンクをアクセスリンクに変更すると、まずそのアクセスリンクより、そのリンク上のIPアドレス（C o A : Care-of Address）を取得する。これは通常、アクセスルータから定期的にアクセスリンク上の全端末に向けて広告されるルータアドバタイズメント（Router Advertisement）を受信するか、DHCPv6を用いることで実現される。

【0013】

2. Binding UpdateとBinding Acknowledgement

次に、移動端末は、自分のホームエージェントに対して、その移動端末のホームアドレスとC o Aとの組を報告する（Binding Update）。報告を受けたホームエージェントは、その組をテーブルとして保存する。移動端末は接続するリンクを変更する度に、このBinding Updateを行う。ホームエージェントはBinding Updateに対してBinding Acknowledgementを返すが、この過程はBinding Updateにその指示があったときのみ行う。

【0014】

3. IPトンネリング

この後、ホームエージェントは、移動端末と通信中の端末（Correspondent Node）からホームリンク（ホームネットワーク）に届いたパケットのうちのテーブル内に登録されたホームアドレス宛てのパケットを、テーブル内に登録されたC o A宛てのIPパケット内のペイロード部分に挿入し、登録されているC o A宛てのIPヘッダを付加して、IPネットワークに転送する（IPトンネリング）。転送されたパケットはIPヘッダのC o Aに従ってアクセスリンク上に届き、そこから移動端末に配送される。移動端末は、そのパケットのペイロード部分を取得することにより、アクセスリンクに接続しながら、ホームアドレス宛てのパケットを受け取ることができる。

【0015】

しかしながら、IPv6では、移動端末が接続するリンクを変更した場合、Binding Updateが完了するまでの間は、以前接続していたリンク（接続変更前に接続していたリンク）に、自分のホームアドレス宛てのパケットが届いてしまうことになり、この間は新しい接続リンク先で自分のホームアドレス宛てのパケットを受

け取ることが不可能となる。特に、移動端末からホームエージェントまでのネットワーク上の距離（中継するルータ数、中継データリンクの容量などに依存する距離）が離れている場合には、移動端末がホームエージェントにBinding Updateを行うのに必要な時間が長くなり、移動端末が自分のホームアドレス宛てのパケットを受け取れない時間が長くなってしまうという問題点がある。

【0016】

この問題に対する1つのアプローチとして、後述の非特許文献5に記載されているように、アクセスリンクから比較的近いリンクで構成されたネットワーク上に、新たに移動端末の位置管理を行うサーバを設置し、移動端末がそのネットワーク内でアクセスリンクを変更した場合には、そのサーバに対してCare-of Addressを登録することにより、Binding Update完了までに要する時間を短縮する階層型MobileIPv6（Hierarchical MIPv6: HMIPv6）が、Mobile IP Working Groupで提案され、現在標準化が行われている。なお、このHMIPv6は、MobileIPv6と共存して動作可能である。

【0017】

図10は、従来の技術に係るHMIPv6のシーケンスを示す図である。HMIPv6では、アクセスを提供しているオペレータ64にMAP（Mobility Anchor Point）と呼ばれる移動端末61の比較的狭いリンク内の移動を管理するサーバを設けている。なお、MAPが管理するリンクはMAPドメインと呼ばれ、MAP62は通常、MAPドメイン内の上位ネットワークに近い側に設置される。HMIPv6では、次のような動作によって、移動端末61がMAPドメイン内で移動する場合のBinding過程に必要な時間を短縮することを可能とする。

【0018】

移動端末61が、新たにMAPドメインに入るか、又は、異なるMAPドメインに移動して接続リンクを変更した場合、まずアクセスリンクより、そのリンク上のLCoA（通常のCoA: On-Link CoA）を取得し、さらに移動端末61は、このアクセスリンク上のMAP62のアドレスを取得する。移動端末61は、そのMAP62のアドレスから、移動端末61の別のCoA（RCoA: Regional CoA）を構成する。そして、移動端末61は、自端末のRCoAとLCoAと

の組を、そのMAP 62に対して登録する（内部位置登録）。MAP 62はこの登録に対して、OKの場合には、Binding Acknowledgementを返すとともに、移動端末61に対して、外部への接続サービスを提供する。また、さらに移動端末61は、自端末のホームエージェント63に対してRCoAの登録を行う。（位置登録シーケンス）。

【0019】

このような位置登録をしておくことによって、移動端末61が同じMAPドメイン内の異なるリンクに接続を変更した場合には、移動端末61は、MAP 62に対してLCoAの登録のみを行えばよく、ホームエージェント63へのLCoAの登録は不要となる。したがって、移動端末61がMAPドメイン内を移動する場合であれば、ホームエージェント63にCoAを登録（Binding Update）し、その確認（Binding Acknowledgement）を受信する一連のBinding過程は省略され、ホームアドレス宛てのパケットを受信できない時間が短縮される。

【0020】

すなわち、HMIPv6では、移動端末61が新たにMAPドメイン内のリンクに接続するか、MAPドメインを変更する場合には、移動端末61は、MAP 62へのRCoAとLCoAとの組の登録、及び、ホームエージェント63へのRCoAの登録が必要となるが、移動端末61がMAPドメイン内で接続リンクを変更する場合には、MAP 62へのLCoAの登録のみを行えばよく、MAPドメイン内での移動時のBinding過程に要する時間を短縮するのに有効である。

【0021】

【非特許文献1】

IEEE 802.1 Working Group, "Port-Based Network Access Control", IEEE 802.1x Standard, June 2001.

【非特許文献2】

Pat R. Calhoun, Tony Johansson, etc., "Diameter Mobile IPv4 Application", Internet Draft, draft-ietf-aaa-diameter-mobileip-13, Oct 2002, Work In Progress.

【非特許文献3】

Perkins. C, "Mobility Support for IPv4", RFC3220, Jan 2002

【非特許文献 4】

C. Perkins, Jari A., etc., "Mobility Support in IPv6", Internet Draft, draft-ietf-mobileip-ipv6-18, Jun 2002, Work In Progress.

【非特許文献 5】

H. Soliman, C. Castelluccia, etc., "Hierarchical Mobile IPv6 mobility management (HMIPv6)" Internet Draft, draft-ietf-mobileip-hmipv6-07, Oct 2002, Work In Progress.

【0 0 2 2】

【発明が解決しようとする課題】

MobileIPv6及びHMIPv6を実際に用いる場合、アクセスを提供しているオペレータと利用者のオペレータとは異なる場合が多く、リンク接続を試みる移動端末に対して認証を行う必要性がある。このためには、移動端末に対して、IP網の所定のネットワークとの接続サービスを提供する前に、サービスを提供するオペレータが、移動端末から認証情報を取得し、その認証情報を用いて認証処理を行い、認証結果に応じて、接続サービスを提供するか否かを決定する必要がある。

【0 0 2 3】

現在、これらの処理を行う条件を満たすものとしては、IEEE802.1xなどのIPレベルでの接続を確立するより前に認証を行う技術が挙げられるが、端末の認証の間や、Binding過程（Binding Update及びBinding Acknowledgementのやり取り）が完了するまでの間、移動端末にはIP網からのパケットが届かないことになってしまい、シームレスハンドオーバを実現することは困難となっている。

【0 0 2 4】

上記課題に鑑み、本発明は、移動端末がリンク接続を変更するハンドオーバ時に、スムーズにハンドオーバを行えるようにするとともに、リンク接続の変更に要する時間を短縮することを可能とする無線通信管理システム及び無線通信管理サーバを提供することを目的とする。

【0 0 2 5】

【課題を解決するための手段】

上記目的を達成するため、本発明では、HMI P v 6 を用いて移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法に関し、移動端末のリンク接続を管理するサーバに対して、移動端末が、リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、移動端末のリンク接続の変更に要する時間を短縮するようにしている。

これにより、HMI P v 6 において、移動端末がリンク接続を変更するハンドオーバー時に、認証シーケンスと位置登録シーケンスとを同時に実行し、リンク接続の変更に要する時間を短縮することが可能となる。

【0026】

さらに、本発明では、上記発明に加えて、移動端末が、リンク接続を変更するための情報と、認証に係る情報とを1つの情報として送信し、リンク接続を管理するサーバが、1つの情報から、リンク接続を変更するための情報及び認証に係る情報のそれぞれを取得するようにしている。

これにより、移動端末は、1つの情報の送信を行うだけで、認証要求及び位置登録要求を行うことが可能となる。

【0027】

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、認証に係る情報を用いた認証処理による認証結果を取得するようにしている。

これにより、認証要求及び位置登録要求を受けたサーバが、認証結果の取得を行うことが可能となる。

【0028】

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末の認証を行う認証サーバとの通信を行い、認証結果を取得するようにしている。

これにより、認証要求及び位置登録要求を受けたサーバが、認証サーバに認証依頼を送信し、認証サーバでの認証結果を受信することが可能となる。

【0029】

さらに、本発明では、上記発明に加えて、移動端末のリンク接続の変更を確認した旨を通知する情報と、認証結果とを1つの情報として、移動端末に送信する

ようにしている。

これにより、1つの情報の送信によって、認証要求及び位置登録要求を受けたサーバが、移動端末に対してリンク接続の変更の確認情報と認証結果とを送信できるようになるとともに、認証結果の送信タイミングを定めることが可能となる。

【0030】

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末のリンク接続の変更を確認した旨を通知する情報を移動端末に送信し、その後、認証結果を取得できた場合に認証結果を移動端末に送信するようにしている。

これにより、認証要求及び位置登録要求を受けたサーバは、時間がかかると予想される認証結果の取得を待つことなく、まず、リンク接続の変更の確認情報を移動端末に返すことが可能となる。

【0031】

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、認証結果の取得までの時間を設定し、認証結果の取得までの時間内に認証結果を取得できた場合、次に移動端末からリンク接続を変更するための情報を受信した際に、移動端末のリンク接続の変更を確認した旨を通知する情報と共に、認証結果を移動端末に送信するようにしている。

これにより、認証要求及び位置登録要求を受けたサーバが認証結果を取得した場合に、移動端末に対して認証結果を送信するタイミングを定めることが可能となる。

【0032】

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末が所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定し、移動端末のリンク接続の変更を確認した旨を通知する情報と共に、所定の時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するようにしている。

これにより、認証処理が終わっていない移動端末に対しても接続許可が与えら

れ、認証処理が完了するのを待つことなく移動端末は、通信を継続することが可能となる。

【0033】

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、所定の仮許可時間よりも長い時間であって、移動端末が所望のネットワークへのアクセスを許可する所定の許可時間を設定し、認証結果が認証成功であった場合、移動端末のリンク接続の変更を確認した旨を通知する情報と共に、所定の許可時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するようにしている。

これにより、認証に成功した移動端末に対しては、十分に長い有効時間が設定された接続許可を与えることが可能となる。

【0034】

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、所定の仮許可時間又は所定の許可時間だけ所望のネットワークへのアクセスを許可した移動端末のリンク接続の変更に係る登録を行い、所定の仮許可時間又は所定の許可時間が経過した場合、移動端末のリンク接続の変更に係る登録を削除するようにしている。

これにより、認証が行われている時間だけ移動端末に与えられていた接続許可や、十分に長い時間だけ移動端末に与えられていた接続許可の有効時間が切れた場合、移動端末をリンクから離すことによって、不正なリンク接続が起こらないようにすることが可能となる。

【0035】

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、認証結果の取得までの時間を設定し、認証結果の取得までの時間内に認証結果を取得できなかった場合、認証結果を認証失敗とするようにしている。

これにより、例えば、認証サーバとの通信が不可能となり、移動端末に係る認証結果が取得できない場合に、移動端末に対して、接続許可を与えないようにすることが可能となる。

【0036】

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末に対して所定の接続禁止時間を設定し、移動端末に対して認証結果として認証失敗を通知した場合には、認証失敗の通知から所定の接続禁止時間だけ、認証失敗であった移動端末のリンク接続の変更に係る処理及び認証に係る処理を行わないようにしている。

これにより、認証に失敗した移動端末に対して、所定の時間だけ接続禁止の設定を行い、リンク接続の変更要求や認証要求を受けないようにすることで、特に、繰り返し行われる不正なアクセスを防止することが可能となる。

【0037】

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末に対して認証結果として認証成功を通知した場合のみ、認証成功であった移動端末のリンク接続の変更に係る登録を行うようにしている。

これにより、認証に成功した移動端末のアドレスのみを登録することが可能となる。

【0038】

また、上記目的を達成するため、本発明では、移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法に関し、移動端末のリンク接続を管理するサーバに対して、移動端末が、リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、リンク接続を管理するサーバが、認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定し、認証結果の取得までの時間内に認証結果を取得できた場合、認証結果を前記移動端末に送信するようにしている。

これにより、認証要求を受けたサーバが認証結果を取得した場合に、移動端末に対して認証結果を送信するタイミングを定めることが可能となる。

【0039】

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末が所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定し、所定の時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するようにしている。

これにより、認証処理が終わっていない移動端末に対しても接続許可が与えられ、認証処理が完了するのを待つことなく移動端末は、通信を継続することが可能となる。

【0040】

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、所定の仮許可時間よりも長い時間であって、移動端末が所望のネットワークへのアクセスを許可する所定の許可時間を設定し、認証結果が認証成功であった場合、所定の許可時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するようにしている。

これにより、認証に成功した移動端末に対しては、十分に長い有効時間が設定された接続許可を与えることが可能となる。

【0041】

さらに、本発明では、上記発明に加えて、所定の仮許可時間又は所定の許可時間が経過した場合、リンク接続を管理するサーバは、移動端末の接続を切断するようにしている。

これにより、認証が行われている時間だけ移動端末に与えられていた接続許可や、十分に長い時間だけ移動端末に与えられていた接続許可の有効時間が切れた場合、移動端末をリンクから離す（ネットワークから切断する）ことによって、不正なリンク接続が起こらないようにすることが可能となる。

【0042】

また、上記目的を達成するため、本発明では、上記発明に加えて、移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法に関し、移動端末のリンク接続を管理するサーバに対して、移動端末が、リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、リンク接続を管理するサーバが、認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定し、認証結果の取得までの時間内に認証結果を取得できなかった場合、認証結果を認証失敗とするようにしている。

これにより、例えば、認証サーバとの通信が不可能となり、移動端末に係る認証結果が取得できない場合に、移動端末に対して、接続許可を与えないようにす

ることが可能となる。

【0043】

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末に対して所定の接続禁止時間を設定し、移動端末に対して認証結果として認証失敗を通知した場合には、認証失敗の通知から所定の接続禁止時間だけ、認証失敗であった移動端末に係る処理を行わないようにしている。

これにより、認証に失敗した移動端末に対して、所定の時間だけ接続禁止の設定を行い、リンク接続の変更要求や認証要求を受けないようにすることで、特に、繰り返し行われる不正なアクセスを防止することが可能となる。

【0044】

さらに、本発明では、上記発明に加えて、リンク接続を管理するサーバが、移動端末に対して認証結果として認証成功を通知した場合のみ、認証成功であった移動端末のリンク接続の変更に係る登録を行うようにしている。

これにより、認証に成功した移動端末のアドレスのみに接続許可を与えることが可能となる。

【0045】

また、上記目的を達成するため、本発明では、HMI P v 6 を用いて移動端末のリンク接続を管理する無線通信管理サーバに関し、移動端末から、リンク接続を変更するための情報と所望のネットワークにアクセスするための認証に係る情報とを1つの情報で受信し、1つの情報から、リンク接続を変更するための情報及び認証に係る情報のそれぞれを取得するよう構成している。

この構成により、移動端末は、1つの情報の送信を行うだけで、認証要求及び位置登録要求を行うことが可能となる。

【0046】

さらに、本発明では、上記発明に加えて、認証に係る情報を用いた認証処理による認証結果を取得するよう構成している。

この構成により、認証要求及び位置登録要求を受けたサーバが、認証結果の取得を行うことが可能となる。

【0047】

さらに、本発明では、上記発明に加えて、移動端末の認証を行う認証サーバとの通信を行う手段を有し、認証結果を取得するよう構成している。

この構成により、認証要求及び位置登録要求を受けたサーバが、認証サーバに認証依頼を送信し、認証サーバでの認証結果を受信することが可能となる。

【0048】

さらに、本発明では、上記発明に加えて、移動端末のリンク接続の変更を確認した旨を通知する情報と認証結果とを1つの情報として、移動端末に送信するよう構成している。

この構成により、1つの情報の送信によって、認証要求及び位置登録要求を受けたサーバが、移動端末に対してリンク接続の変更の確認情報と認証結果とを送信できるようになるとともに、認証結果の送信タイミングを定めることが可能となる。

【0049】

さらに、本発明では、上記発明に加えて、移動端末のリンク接続の変更を確認した旨を通知する情報を移動端末に送信し、その後、認証結果を取得できた場合に認証結果を移動端末に送信するよう構成している。

この構成により、認証要求及び位置登録要求を受けたサーバは、時間がかかると予想される認証結果の取得を待つことなく、まず、リンク接続の変更の確認情報を移動端末に返すことが可能となる。

【0050】

さらに、本発明では、上記発明に加えて、認証結果の取得までの時間を設定する時間設定手段を有し、認証結果の取得までの時間内に認証結果を取得できた場合、次に移動端末からリンク接続を変更するための情報を受信した際に、移動端末のリンク接続の変更を確認した旨を通知する情報と共に、認証結果を移動端末に送信するよう構成している。

この構成により、認証要求及び位置登録要求を受けたサーバが認証結果を取得した場合に、移動端末に対して認証結果を送信するタイミングを定めることが可能となる。

【0051】

さらに、本発明では、上記発明に加えて、移動端末に対して所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定する時間設定手段を有し、移動端末のリンク接続の変更を確認した旨を通知する情報と共に、所定の時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するよう構成している

この構成により、認証処理が終わっていない移動端末に対しても接続許可が与えられ、認証処理が完了するのを待つことなく移動端末は、通信を継続することが可能となる。

【0052】

さらに、本発明では、上記発明に加えて、移動端末に対して、所定の仮許可時間よりも長い時間であって、移動端末が所望のネットワークへのアクセスを許可する所定の許可時間を設定する時間設定手段を有し、認証結果が認証成功であった場合、移動端末のリンク接続の変更を確認した旨を通知する情報と共に、所定の許可時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するよう構成している。

この構成により、認証に成功した移動端末に対しては、十分に長い有効時間が設定された接続許可を与えることが可能となる。

【0053】

さらに、本発明では、上記発明に加えて、所定の仮許可時間又は所定の許可時間だけ所望のネットワークへのアクセスを許可した移動端末のリンク接続の変更に係る登録を行う情報登録手段と、所定の仮許可時間又は所定の許可時間が経過した場合、移動端末のリンク接続の変更に係る登録を削除する情報削除手段とを有するよう構成している。

この構成により、認証が行われている時間だけ移動端末に与えられていた接続許可や、十分に長い時間だけ移動端末に与えられていた接続許可の有効時間が切れた場合、移動端末をリンクから離すことによって、不正なリンク接続が起こらないようにすることが可能となる。

【0054】

さらに、本発明では、上記発明に加えて、認証結果の取得までの時間を設定す

る時間設定手段と、認証結果の取得までの時間内に認証結果を取得できなかった場合、認証結果を認証失敗とする判定手段とを有するよう構成している。

この構成により、例えば、認証サーバとの通信が不可能となり、移動端末に係る認証結果が取得できない場合に、移動端末に対して、接続許可を与えないようにすることが可能となる。

【0055】

さらに、本発明では、上記発明に加えて、移動端末に対して所定の接続禁止時間を設定する時間設定手段と、移動端末に対して認証結果として認証失敗を通知した場合には、認証失敗の通知から所定の接続禁止時間だけ、認証失敗であった移動端末のリンク接続の変更に係る処理及び認証に係る処理を行わないよう制御する制御手段とを有するよう構成している。

この構成により、認証に失敗した移動端末に対して、所定の時間だけ接続禁止の設定を行い、リンク接続の変更要求や認証要求を受けないようにすることで、特に、繰り返し行われる不正なアクセスを防止することが可能となる。

【0056】

さらに、本発明では、上記発明に加えて、移動端末に対して認証結果として認証成功を通知した場合のみ、認証成功であった移動端末のリンク接続の変更に係る登録を行うよう制御する制御手段を有するよう構成している。

この構成により、認証に成功した移動端末のアドレスのみを登録することが可能となる。

【0057】

また、上記目的を達成するため、本発明では、移動端末のリンク接続を管理する無線通信管理サーバに関し、移動端末から、リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を受信する受信手段と、認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定する時間設定手段と、認証結果の取得までの時間内に認証結果を取得できた場合、認証結果を移動端末に送信する送信手段とを有している。

この構成により、認証要求を受けたサーバが認証結果を取得した場合に、移動端末に対して認証結果を送信するタイミングを定めることが可能となる。

【0058】

さらに、本発明では、上記発明に加えて、移動端末が所望のネットワークへのアクセスを仮許可する所定の仮許可時間を設定する時間設定手段を有し、所定の時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するよう構成している。

この構成により、認証処理が終わっていない移動端末に対しても接続許可が与えられ、認証処理が完了するのを待つことなく移動端末は、通信を継続することが可能となる。

【0059】

さらに、本発明では、上記発明に加えて、所定の仮許可時間よりも長い時間であって、移動端末が所望のネットワークへのアクセスを許可する所定の許可時間を設定する時間設定手段を有し、認証結果が認証成功であった場合、所定の許可時間だけ所望のネットワークへのアクセスの許可を通知する情報を移動端末に送信するよう構成している。

この構成により、認証に成功した移動端末に対しては、十分に長い有効時間が設定された接続許可を与えることが可能となる。

【0060】

さらに、本発明では、上記発明に加えて、所定の仮許可時間又は所定の許可時間が経過した場合、移動端末の接続を切断する制御手段を有している。

この構成により、認証が行われている時間だけ移動端末に与えられていた接続許可や、十分に長い時間だけ移動端末に与えられていた接続許可の有効時間が切れた場合、移動端末をリンクから離す（ネットワークから切断する）ことによって、不正なリンク接続が起こらないようにすることが可能となる。

【0061】

また、上記目的を達成するため、本発明では、移動端末のリンク接続を管理する無線通信システムにおける無線通信管理サーバに関し、移動端末から、リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を受信する受信手段と、リンク接続を管理するサーバが、認証に係る情報を用いた認証処理による認証結果の取得までの時間を設定する時間設定

手段と、認証結果の取得までの時間内に認証結果を取得できなかった場合、認証結果を認証失敗として、認証結果を移動端末に送信する送信手段とを有している。

この構成により、例えば、認証サーバとの通信が不可能となり、移動端末に係る認証結果が取得できない場合に、移動端末に対して、接続許可を与えないようにすることが可能となる。

【0062】

さらに、本発明では、上記発明に加えて、移動端末に対して所定の接続禁止時間を設定する時間設定手段と、移動端末に対して認証結果として認証失敗を通知した場合には、認証失敗の通知から所定の接続禁止時間だけ、認証失敗であった移動端末に係る処理を行わないよう制御する制御手段とを有している。

この構成により、認証に失敗した移動端末に対して、所定の時間だけ接続禁止の設定を行い、リンク接続の変更要求や認証要求を受けないようにすることで、特に、繰り返し行われる不正なアクセスを防止することが可能となる。

【0063】

さらに、本発明では、上記発明に加えて、移動端末に対して認証結果として認証成功を通知した場合のみ、認証成功であった移動端末のリンク接続の変更に係る登録を行うよう制御する制御手段を有している。

この構成により、認証に成功した移動端末のみを接続許可を与えることが可能となる。

【0064】

【発明の実施の形態】

以下、図面を参照しながら、本発明の実施の形態について説明する。

(第1の実施の形態)

まず、図面を参照しながら、本発明の第1の実施の形態について説明する。本発明の第1の実施の形態では、HMIP v 6 (Hierarchical Mobile IP version 6) の位置登録シーケンス中に認証シーケンスを含めることによって、ハンドオーバーに要する時間を短縮し、シームレスな接続サービスを提供することを可能とする技術について説明する。

【0065】

図1は、本発明の第1の実施の形態におけるMAPの構成を示すブロック図である。図1に示すMAP (Mobility Anchor Point) 10は、上位ネットワーク20と接続する上位ネットワーク通信手段11、下位ネットワーク25と接続する下位ネットワーク通信手段12、HMIPv6を利用したデータ伝送の経路を決定及び制御するHMIPv6経路制御手段13、認証サーバ32に対して認証要求の送信及び認証結果の受信を行う認証要求送受信手段14、データ伝送経路の設定の際に参照されるHMIPv6テーブル16と認証サーバ32のアドレス17とを格納する情報格納手段15を有している。このうち、本発明の第1の実施の形態に特徴的な構成要素は認証要求送受信手段14と、情報格納手段15に格納された認証サーバ32のアドレス17であり、上位ネットワーク通信手段11、下位ネットワーク通信手段12、HMIPv6経路制御手段13は、従来から存在するものを利用することが可能である。なお、MAP10はコンピュータによって実現可能であり、上記の各手段はCPUなどの中央処理手段によって実現可能であるとともに、様々な情報の参照し、判断・判定処理を行うことも可能である。

【0066】

図2は、本発明の第1の実施の形態におけるシーケンスを示す図である。図2には、利用者がネットワークと接続して通信を行うために利用する移動端末21、移動端末21によるネットワークへのアクセスを提供しているオペレータ30、利用者のオペレータ40が図示されている。また、アクセスを提供しているオペレータ30には、アクセスルータ31、MAP10、認証サーバ32が存在し、利用者のオペレータ40には、ホームエージェント41、認証サーバ42が存在する。なお、図2におけるMAP10は、図1に示す本発明を実施するためのMAP10である。

【0067】

まず、移動端末21が新たなリンクに接続した場合、移動端末21はアクセスルータ31に対して、ルータアドバタイズメント (Router Advertisement) の送信を促すルータソリシテーション (Router Solicitation) を送信する (ステ

ップS101)。このルータソリシテーションを受けて、アクセスルータ31は移動端末21に対して、IPアドレスなどのルータ情報を含むルータアドバタイズメントを送信する(ステップS102)。なお、アクセスルータ31がルータソリシテーションを受けずに、マルチキャストで定期的にルータアドバタイズメントを流すことも可能である。

【0068】

移動端末21は、アクセスルータ31からのルータアドバタイズメントを受けて、接続したリンク上のIPアドレス(LCoA: On-link Care-of Address)を取得する。また、移動端末21の接続したリンクがMAP10ドメイン内のリンクである場合、このリンクでのMAP10の利用が可能であることがルータアドバタイズメントに示されており、HMIPv6を搭載した移動端末21は、MAP10のアドレスを取得することが可能である。そして、このMAP10のアドレスから、もう1つのCoAであるRCoA(Regional Care-of Address)を構成する。

【0069】

次に、HMIPv6を実装する移動端末21は、MAP10へのBinding Update(バインディングアップデート: なお、BUと省略することもある)を行うための情報(LCoA)と、端末ID及び利用者情報を含む認証情報とを、MAP10に対して送信する(ステップS103)。MAP10は、情報格納手段15内に格納されている認証サーバ32のアドレス17を参照し、認証要求送受信手段14を用いて、認証サーバ32に対して認証要求を送信する(ステップS104)。また、必要ならば、アクセスを提供しているオペレータ30の認証サーバ32は、利用者のオペレータ40の認証サーバ42に対して認証依頼を送信し(ステップS105)、認証処理後の応答(認証結果)を受信する(ステップS106)。そして、認証サーバ32はMAP10に対して、認証結果を返す(ステップS107)。

【0070】

なお、上記のステップS106及びステップS107の処理が必要でない場合(アクセスを提供しているオペレータ30の認証サーバ32において、認証処理

が可能な場合) には、アクセスを提供しているオペレータ 30 の認証サーバ 32 で認証処理を行って、その認証結果を MAP 10 に返すようにする。また、MAP 10 が、利用者のオペレータ 40 の認証サーバ 42 と認証依頼及び認証結果のやり取りを直接行うことも可能である。

【0071】

一方、MAP 10 は、認証サーバ 32 への認証要求の送信と同時に RCOA 及び LCOA の登録 (Binding Update) を行う。MAP 10 は、RCOA 及び LCOA の登録が完了し、かつ、認証サーバ 32 から認証結果を受けた時点で、Binding Acknowledgement (バインディングアクノレッジメント: なお、BA と省略することもある) と認証結果とを移動端末 21 に対して送信する (ステップ S108)。

【0072】

上記までの動作が終了すると、その後は従来と同様の HMIPv6 におけるホームエージェント 41 への Binding Update が行われる。すなわち、移動端末 21 は、RCOA をホームエージェント 41 に送信して、ホームエージェント 41 から登録されたことを示す Binding Acknowledgement を受信する。

【0073】

以上、説明したように、本発明の第 1 の実施の形態によれば、シームレスハンドオーバを目的とし、すでに標準化が進められている HMIPv6 の位置登録シーケンス中に、認証シーケンスを含めることによって、IP アドレスの移動に係る制御と同時に認証処理を行うことが可能となり、位置登録シーケンスと認証シーケンスが独立に行われていた場合に比べて、ハンドオーバに要する時間が短縮し、移動端末 21 に対してシームレスな接続サービスを提供することが可能となる。

【0074】

(第 2 の実施の形態)

次に、図面を参照しながら、本発明の第 2 の実施の形態について説明する。本発明の第 2 の実施の形態では、HMIPv6 の位置登録シーケンス中に認証シーケンスを含め、さらに、認証処理にかかる時間 (認証時間) を考慮して、その認

証時間中においても、移動端末 21 がネットワークにアクセスできるようにすることによって、ハンドオーバーに要する時間を短縮し、シームレスな接続サービスを提供することを可能とする技術について説明する。

【0075】

これは、特に、アクセスを提供しているオペレータ 30 に属するアクセスネットワークと利用者のオペレータに属するホームネットワークとが異なっており、MAP 10 が認証サーバ 32、42 に対して認証依頼を行ってから認証結果が返ってくるまでの時間が長い場合に有効である。このように認証時間が長くなる理由は、アクセスネットワークとホームネットワークとが離れていることに加え、以下の理由による。

【0076】

移動端末 21 がアクセスネットワークに接続するためには、まず、アクセスネットワークとホームネットワークとが、互いにローミング契約をしている必要があるが、この場合、移動端末 21 はアクセスネットワークにとってはローミング端末となるため、アクセスネットワーク内の認証サーバ 32 が当該移動端末 21 の認証情報を有さないことがある。この場合、通常、アクセスを提供しているオペレータ 30 に属する認証サーバ 32（アクセスネットワーク上の認証サーバ 32）が利用者のオペレータ 30 に属する認証サーバ 42（ホームネットワーク上の認証サーバ 42）に対して移動端末 21 の認証依頼を行う。なお、このような認証情報転送機構は、各オペレータ間のローミング契約や認証サーバ間のプロトコルなどに依存するものである。

【0077】

図 3 は、本発明の第 2 の実施の形態における MAP の構成を示すブロック図である。図 3 に示す MAP 10 は、上位ネットワーク 20 と接続する上位ネットワーク通信手段 11、下位ネットワーク 25 と接続する下位ネットワーク通信手段 12、HMI P v 6 を利用したデータ伝送の経路を決定及び制御する HMI P v 6 経路制御手段 13、認証サーバ 32 に対して認証要求の送信及び認証結果の受信を行う認証要求送受信手段 14、データ伝送経路の設定の際に参照される HMI P v 6 テーブル（RC o A / LC o A テーブルを含む）16、認証サーバ 32

のアドレス 17、状態テーブル 19 を格納する情報格納手段 15、時間管理手段 18 を有している。

【0078】

このうち、本発明の第 1 の実施の形態に加えて特徴的な構成要素は時間管理手段 18 と、情報格納手段 15 に格納された状態テーブル 19 であり、上位ネットワーク通信手段 11、下位ネットワーク通信手段 12、HMIP v6 経路制御手段 13、認証要求送受信手段 14 は、本発明の第 1 の実施の形態で存在するものを利用することが可能である。なお、MAP 10 はコンピュータによって実現可能であり、上記の各手段は CPU などの中央処理手段によって実現可能であるとともに、様々な情報の参照し、判断・判定処理を行うことも可能である。

【0079】

時間管理手段 18 は、主に、時間を計測する計時機能と、計時結果に従って所定の値を減算（後述の図 6 に示す状態テーブル 19 中の設定値をスタート値とするカウントダウン）し、残り時間が 0 になったか否かを判定する残り時間判定機能を有している。また、様々な時間情報の設定を行う時間設定手段としての機能も有している。なお、所定の時間が経過したか否かの判定が可能であれば、残り時間判定機能のほかに、所定の時間が経過したか否かを判定する機能、又は、所定の時刻に達したか否かを判定する機能を用いることも可能である。

【0080】

図 4 は、本発明の第 2 の実施の形態におけるシーケンスを示す図である。図 4 には、図 2 と同様、移動端末 21、アクセスを提供しているオペレータ 30、利用者のオペレータ 40 が図示されており、アクセスを提供しているオペレータ 30 には、アクセスルータ 31、MAP 10、認証サーバ 32 が存在し、利用者のオペレータ 40 には、ホームエージェント 41、認証サーバ 42 が存在する。なお、図 4 における MAP 10 は、図 3 に示す本発明を実施するための MAP 10 である。

【0081】

第 1 の実施の形態と同様、移動端末 21 が新たなリンクに接続した場合、移動端末 21 はアクセスルータに対して、ルータソリシテーションを送信し（ステッ

プ S 2 0 1)、これを受けて、アクセスルータは移動端末 2 1 に対して、ルータアドバタイズメントを送信する(ステップ S 2 0 2)。そして、移動端末 2 1 は、アクセスルータからのルータアドバタイズメントを受けて、接続したリンク上の L C o A と M A P 1 0 のアドレスとを取得し、R C o A を構成する。

【0082】

次に、H M I P v 6 を実装する移動端末 2 1 は、M A P 1 0 への Binding Update を行うため、L C o A と、端末 I D 及び利用者情報を含む認証情報とを、M A P 1 0 に対して送信する(ステップ S 2 0 3)。M A P 1 0 は、この Binding Update に関して R C o A 及び L C o A の登録を行い、移動端末 2 1 に対して、十分に短い接続の有効時間(仮 Binding 有効時間 T 1)を設定して Binding Acknowledgement を返信する(ステップ S 2 0 4)。なお、この Binding Acknowledgement は、仮 Binding 有効時間 T 1 だけネットワークへの接続許可を与えるものであり、すなわち、この Binding Acknowledgement を受けた移動端末 2 1 は、仮 Binding 有効時間 T 1 だけネットワークに接続することが可能となる。

【0083】

さらに、M A P 1 0 は、情報格納手段 1 5 内に格納されている認証サーバ 3 2 のアドレス 1 7 を参照し、認証要求送受信手段 1 4 を用いて、認証サーバ 3 2 に対して認証要求を送信する(ステップ S 2 0 5)。また、必要ならば、アクセスを提供しているオペレータ 3 0 の認証サーバ 3 2 は、利用者のオペレータ 4 0 の認証サーバ 4 2 に対して認証依頼を送信し(ステップ S 2 0 6)、認証処理後の応答(認証結果)を受信する(ステップ S 2 0 7)。そして、認証サーバ 3 2 は M A P 1 0 に対して、認証結果を返す(ステップ S 2 0 8)。

【0084】

なお、第 1 の実施の形態と同様、上記のステップ S 2 0 6 及びステップ S 2 0 7 の処理が必要でない場合(アクセスを提供しているオペレータ 3 0 の認証サーバ 3 2 において、認証処理が可能な場合)には、アクセスを提供しているオペレータ 3 0 の認証サーバ 3 2 で認証処理を行って、その認証結果を M A P 1 0 に返すようにする。また、M A P 1 0 が、利用者のオペレータ 4 0 の認証サーバ 4 2 と認証依頼及び認証結果のやり取りを直接行うことも可能である。

【0085】

一方、MAP 10は、仮Binding有効時間T1だけネットワークへの接続が許可された後も、周期的又は仮Binding有効時間T1に達する直前に、MAP 10へのBinding Updateを行うための情報(LC o A)と、端末ID及び利用者情報を含む認証情報とを、MAP 10に対して送信する(ステップS209)。

【0086】

このステップS209におけるBinding Updateを受けた時点で、ステップS208における認証サーバ32からの認証結果の受信が完了している場合には、MAP 10は、Binding Acknowledgementと認証結果とを移動端末21に対して送信する(ステップS210)。このとき、認証結果が成功を示すものである場合には、MAP 10は、移動端末21に対して、接続許可及び仮Binding有効時間T1に比べて十分長いBinding有効時間T2を送信する。このBinding Acknowledgementを受けた移動端末21は、Binding有効時間T2だけネットワークに接続することが可能となる。その後は、従来と同様のHMIPv6におけるホームエージェント41へのBinding Updateが行われ、移動端末21がRC o Aをホームエージェント41に送信し、ホームエージェント41から登録完了を示すBinding Acknowledgementを受信する。

【0087】

一方、図4には不図示だが、ステップS209におけるBinding Updateを受けた時点で、ステップS208における認証サーバ32からの認証結果の受信が完了していない場合(認証結果の受信前に移動端末21からBinding Updateを再受信した場合)には、MAP 10は、再びステップS204に戻り、移動端末21に対して仮Binding有効時間T1だけネットワークへの接続許可を与えるBinding Acknowledgementを送信する。なお、移動端末21に対して仮Binding有効時間T1だけネットワークへの接続許可を与えるBinding Acknowledgementを送信する処理は、認証サーバ32から認証結果を受信するまで繰り返される。

【0088】

さらに、図4には不図示だが、所定の認証要求有効時間Taが経過しても、認証サーバ32から認証結果を受信することができなかった場合(すなわち、ステ

ップS208の処理が行われなかった場合)には、MAP10は、当該移動端末21の認証が失敗したとみなして、移動端末21に対して認証失敗を示す認証結果を送信するとともに、所定の認証要求再開時間 T_r の間は接続禁止期間(接続禁止時間)とし、当該移動端末21からのBinding Updateに対して、接続禁止期間であることを示すBinding Acknowledgementを返すようにする。

【0089】

また、上記のシーケンスにおいて、移動端末21からBinding Updateを受けた際のMAP10の処理の詳細について説明する。図5は、本発明の第2の実施の形態における移動端末からBinding Updateを受けた際のMAPの処理の詳細を示すフローチャートである。MAP10は、移動端末21からBinding Updateを受信し(ステップS301)、状態テーブル19に当該Binding Updateの送信元の移動端末21のLCOAが存在しているか否かを調べる(ステップS302)。

【0090】

また、図6は、本発明の第2の実施の形態における状態テーブルの一例を示す模式図である。図6に示されているように、状態テーブル19には、移動端末21のLCOA、認証結果、認証要求有効時間 T_a の設定値、認証要求再開時間 T_r の設定値、仮Binding時間 T_1 の設定値、Binding時間 T_2 の設定値の組み合わせが記録される。なお、認証結果は、この移動端末21の認証処理における状態や認証結果を含むものであり、例えば、現在認証処理中であることを示す「処理中」、認証に成功したことを示す「認証成功」、認証に失敗したことを示す「認証失敗」、接続が禁止されていることを示す「禁止」などが挙げられる。また、仮Binding時間 T_1 及び認証要求有効時間 T_a は認証処理中の状態で付与されるもの、Binding時間 T_2 は認証成功の状態で付与されるもの、認証要求再開時間 T_r は認証失敗の状態で付与されるものである。

【0091】

この移動端末21のLCOAが状態テーブル19に存在していない場合には、この移動端末21のLCOAを状態テーブル19に加えて(ステップS303)、状態テーブル19中の当該LCOAの認証結果を「処理中」にセットする(ステップS304)。そして、当該BU中の認証情報(移動端末21の端末IDや

利用者情報) を基にして、この移動端末 21 の認証処理を行うよう要求する認証要求を認証サーバ 32 に送信し (ステップ S 305)、同時に、当該 LC o A の認証要求有効時間 T a をセットし、カウントダウン (減算処理) を開始する (ステップ S 306)。

【0092】

なお、認証要求有効時間 T a として、認証サーバ 32 とのやり取りや認証サーバ 32 での認証処理にかかる時間より少し長い時間が設定されることが好ましい。また、移動端末 21 や認証サーバ 32 に係る様々な条件を考慮して、認証要求有効時間 T a を移動端末 21 毎 (LC o A 毎) に設定することも可能であり、一律に所定の値に設定することも可能である。

【0093】

そして、RC o A / LC o A テーブルに、この移動端末 21 の RC o A / LC o A の組を追加 (登録) し (ステップ S 307)、当該 LC o A の仮 Binding 時間 T 1 をセットし、カウントダウン (減算処理) を開始する (ステップ S 308)。なお、仮 Binding 時間 T 1 として、その時間内では不正なネットワークアクセスが不可能な程度に短い時間が設定されることが好ましい。また、移動端末 21 や認証サーバ 32 に係る様々な条件を考慮して、仮 Binding 時間 T 1 を移動端末 21 毎 (LC o A 毎) に設定することも可能であり、一律に所定の値に設定することも可能である。このようにして設定された接続許可と、接続が許可される有効時間である仮 Binding 時間 T 1 とを記載した Binding Acknowledgement を当該移動端末 21 に送信し (ステップ S 309)、移動端末 21 や認証サーバ 32 からの応答を受信したり、認証要求有効時間 T a や仮 Binding 時間 T 1 のカウントダウンが 0 になったりする場合まで、待機状態となる。

【0094】

一方、この移動端末 21 の LC o A が状態テーブル 19 に存在している場合には、当該 LC o A の認証結果が「処理中」であるか否かを調べる (ステップ S 310)。当該 LC o A の認証結果が「処理中」である場合には、Binding Acknowledgement 内に「処理中」であることを記載し (ステップ S 311)、当該 LC o A の仮 Binding 時間 T 1 をセットし、新たにカウントダウン (減算処理) を開

始して（ステップS312）、新たに設定された接続許可と、接続が許可される有効時間である仮Binding時間T1とを記載したBinding Acknowledgementを当該移動端末21に送信する（ステップS313）。そして、移動端末21や認証サーバ32からの応答を受信したり、認証要求有効時間Taや仮Binding時間T1のカウンタダウンが0になったりする場合まで、待機状態となる。

【0095】

また、当該LCOAの認証結果が「処理中」でない場合には、当該LCOAの認証結果が「禁止」であるか否かを調べる（ステップS314）。当該LCOAの認証結果が「禁止」である場合には、Binding Acknowledgement内に、接続禁止期間であることを記載して、移動端末21に送信する（ステップS315）。

【0096】

また、当該LCOAの認証結果が「禁止」でない場合には、当該LCOAの認証結果が「認証成功」であるか否かを調べる（ステップS316）。当該LCOAの認証結果が「認証成功」である場合には、RCOA/LCOAテーブルに、この移動端末21のRCOA/LCOAの組を追加（登録）し（ステップS317）、当該LCOAのBinding時間T2をセットし、カウンタダウン（減算処理）を開始する（ステップS318）。なお、Binding時間T2として、移動端末21に十分な接続サービスを提供できる程度に長い時間が設定されることが好ましい。また、移動端末21や認証サーバ32に係る様々な条件を考慮して、Binding時間T2を移動端末21毎（LCOA毎）に設定することも可能であり、一律に所定の値に設定することも可能である。MAP10は、このようにして設定された接続許可と、接続が許可される有効時間であるBinding時間T2とを記載したBinding Acknowledgementを当該移動端末21に送信し（ステップS319）、移動端末21に対して、Binding時間T2の接続サービスを提供する。

【0097】

また、当該LCOAの認証結果が「認証成功」でない場合には、当該LCOAの認証結果は「認証失敗」とみなされ、Binding Acknowledgement内に、認証失敗であることを記載して、移動端末21に送信する（ステップS320）。また、所定の時間（認証要求再開時間Tr）だけの期間、その移動端末21の

認証処理を行わないようにするため、状態テーブル 19 中の当該移動端末 21 の L C o A の認証結果を「禁止」にセットし（ステップ S 3 2 1）、同時に、当該 L C o A の認証要求再開時間 T r をセットし、カウントダウン（減算処理）を開始する（ステップ S 3 2 2）。

【0098】

図 5 に示すフローチャートでは、M A P 10 は、所定の処理を終了して待機状態となる。この待機状態では、M A P 10 は、移動端末 21 や認証サーバ 32 からの応答の受信を待機する状態、仮 Binding 時間 T 1、Binding 時間 T 2、認証要求有効時間 T a、認証要求再開時間 T r のカウントダウンが 0 になるまで待機する状態など、様々な待機状態となっている。この待機状態中に再び移動端末 21 から B U を受信した場合には、図 5 に示すフローチャートに示す処理を繰り返す一方、認証サーバ 32 から認証結果を受信した場合や仮 Binding 時間 T 1、Binding 時間 T 2、認証要求有効時間 T a、認証要求再開時間 T r のカウントダウンが 0 になった場合には、図 7 に示すフローチャートの処理を行う。

【0099】

図 7 は、本発明の第 2 の実施の形態における認証サーバから認証結果を受信した場合及び所定の時間が経過した場合の M A P の処理の詳細を示すフローチャートである。なお、図 7 に示すフローチャートは、図 5 に示すフローチャートから連続したものであり、図 5 に示す待機状態（ステップ S 3 3 3）と図 7 に示す待機状態（ステップ S 3 3 3）は同一ステップである。

【0100】

まず、M A P 10 が、認証サーバ 32 から移動端末 21 の認証結果を受信（ステップ S 3 4 1）した場合、状態テーブル 19 中にその認証処理の対象となった移動端末 21 が存在しているか否か（当該移動端末 21 に係るエントリが存在しているか否か）を調べる（ステップ S 3 4 2）。当該移動端末 21 が存在していない場合には、すでにその移動端末 21 に係る認証処理を行う必要はなく、再び待機状態に戻る。一方、当該移動端末 21 が存在する場合には、認証結果が許可を示すものか否かを判定する（ステップ S 3 4 3）。

【0101】

認証結果が許可を示すものであった場合には、MAP 10 は、状態テーブル 19 中の当該移動端末 21 の認証結果を「認証成功」に設定し（ステップ S 344）、認証成功の場合の処理（ステップ S 317～S 319 までの処理と同一）を行う（ステップ S 345）一方、認証結果が不許可を示すものであった場合には、MAP 10 は、状態テーブル 19 中の当該移動端末 21 の認証結果を「認証失敗」に設定し（ステップ S 346）、認証失敗の場合の処理（ステップ S 320～S 322 までの処理と同一）を行って（ステップ S 347）、再び待機状態に戻る。

【0102】

また、認証要求再開時間 T_r が 0 になった（ステップ S 348）場合には、その移動端末 21 に対する接続禁止区間の設定を終了し、状態テーブル 19 中から、その移動端末 21 に係るエントリを削除する（ステップ S 349）。また、認証要求有効時間 T_a が 0 になった（ステップ S 350）場合には、認証サーバ 32 から認証結果を取得することができず、状態テーブル 19 中の当該移動端末 21 の認証結果を「認証失敗」に設定し（ステップ S 351）、認証失敗の場合の処理（ステップ S 320～S 322 までの処理と同一）を行って（ステップ S 352）、再び待機状態に戻る。

【0103】

また、仮 Binding 時間 T_1 又は Binding 時間 T_2 が 0 になった（ステップ S 353）場合には、その移動端末 21 に提供している接続サービスの有効期限が切れて無効になったとみなし、R C o A / L C o A テーブルから当該移動端末 21 に関する情報を削除して（ステップ S 354）、再び待機状態に戻る。

【0104】

以上、説明したように、本発明の第 2 の実施の形態によれば、シームレスハンドオーバを目的とし、すでに標準化が進められている H M I P v 6 の位置登録シーケンス中に認証シーケンスを含め、さらに、認証シーケンスに時間がかかる場合を考慮して、その認証時間中においても、移動端末 21 がネットワークにアクセスできるようにすることによって、IP アドレスの移動に係る制御と同時に認証処理を行うことが可能となり、位置登録シーケンスと認証シーケンスが独立に

行われていた場合や本発明の第1の実施の形態で説明した位置登録シーケンスと認証シーケンスとを同時に行う技術に比べて、さらに、ハンドオーバーに要する時間が短縮し、移動端末21に対してシームレスな接続サービスを提供することが可能となる。

【0105】

また、上記の第2の実施の形態では、特にHMI Pv6を利用する無線通信システムを例にして説明したが、下記の1～4に示す

1. 短時間だけ仮の接続許可を与えること（上記の仮Binding時間T1に対応）
2. 接続許可に時間制限を設けること（上記のBinding時間T2に対応）
3. 認証サーバに認証要求を行う際にその応答を受けるまでの時間を設定すること（上記の認証要求有効時間Taに対応）
4. 認証に失敗した移動端末に対しては、一定時間だけ接続を禁止すること（上記の認証要求再開時間Trに対応）

は、HMI Pv6に限らず、例えば、グローバルIP v4や、従来の技術で説明したDiameter Mobile IPv4など、他の通信プロトコルを利用する無線通信システムにおいても適用可能である。

【0106】

この場合、上記の第2の実施の形態において、MAP10を管理サーバ、Binding Updateを接続要求、Binding Acknowledgementを接続要求への応答、Binding時間を接続許可時間、LCoAを端末識別情報、RCoA/LCoAテーブルを接続許可テーブルなどとそれぞれ読み換え、状態テーブルとして、図8に示す状態テーブルを用いることにより、HMIPv6以外の通信プロトコルへの一般化が可能である。また、上記の第2の実施の形態では、管理サーバが、認証に成功した移動端末21に対して、すぐに接続サービスを提供するようにしているが、移動端末21からの接続要求があってその認証に成功した場合、まず、状態テーブルに「認証成功」の旨を記載しておき、次に、再び当該移動端末から接続要求を受信した場合に、状態テーブルの「認証成功」の記載を確認して、初めて通常の時間の接続サービスを提供することも可能である。

【0107】

【発明の効果】

以上、説明したように、本発明によれば、HMI P v 6 を用いて移動端末のリンク接続を管理する無線通信システムにおける無線通信管理方法に関し、移動端末のリンク接続を管理するサーバに対して、移動端末が、リンク接続を変更するための情報と同時に、所望のネットワークにアクセスするための認証に係る情報を送信し、位置登録シーケンスと認証シーケンスとを同時に行えるようにしているので、移動端末がリンク接続を変更するハンドオーバー時に、スムーズにハンドオーバーを行えるようにするとともに、リンク接続の変更に要する時間を短縮することが可能となる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施の形態における M A P の構成を示すブロック図

【図 2】

本発明の第 1 の実施の形態におけるシーケンスを示す図

【図 3】

本発明の第 2 の実施の形態における M A P の構成を示すブロック図

【図 4】

本発明の第 2 の実施の形態におけるシーケンスを示す図

【図 5】

本発明の第 2 の実施の形態における移動端末から Binding Update を受けた際の M A P の処理の詳細を示すフローチャート

【図 6】

本発明の第 2 の実施の形態における状態テーブルの一例を示す模式図

【図 7】

本発明の第 2 の実施の形態における認証サーバ 3 2 から認証結果を受信した場合及び所定の時間が経過した場合の M A P の処理の詳細を示すフローチャート

【図 8】

本発明に係る状態テーブルの別の一例を示す模式図

【図 9】

従来の技術に係るDiameter Mobile IPv4 Applicationのシーケンスを示す図

【図 10】

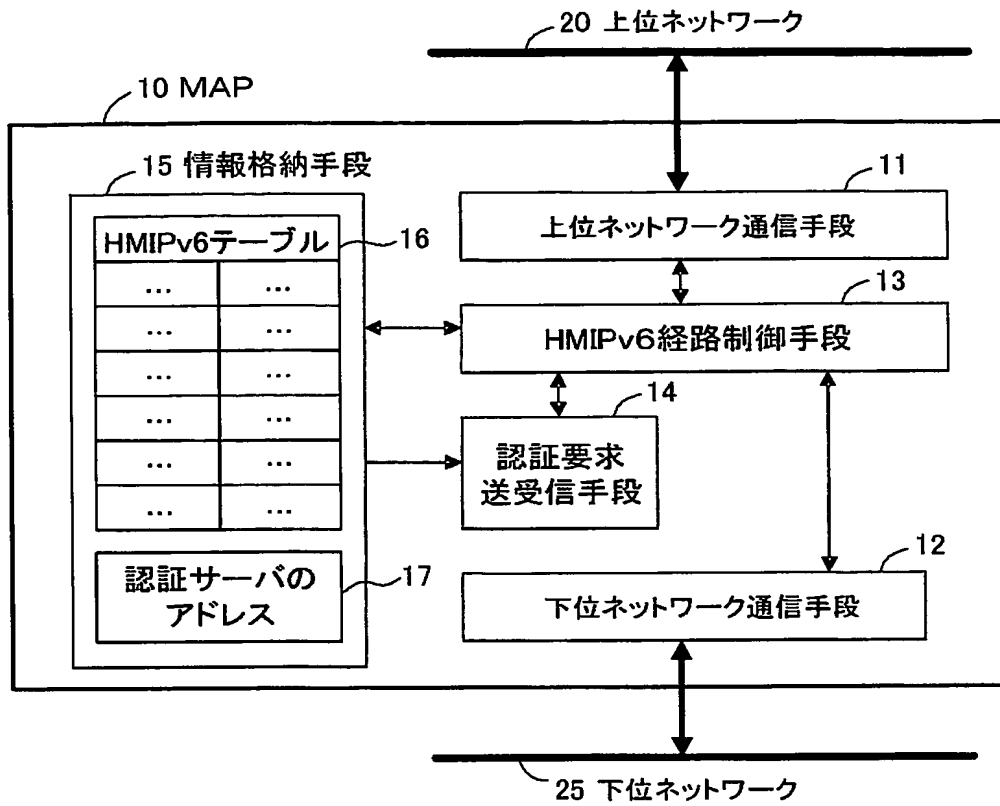
従来の技術に係るHMIPv6のシーケンスを示す図

【符号の説明】

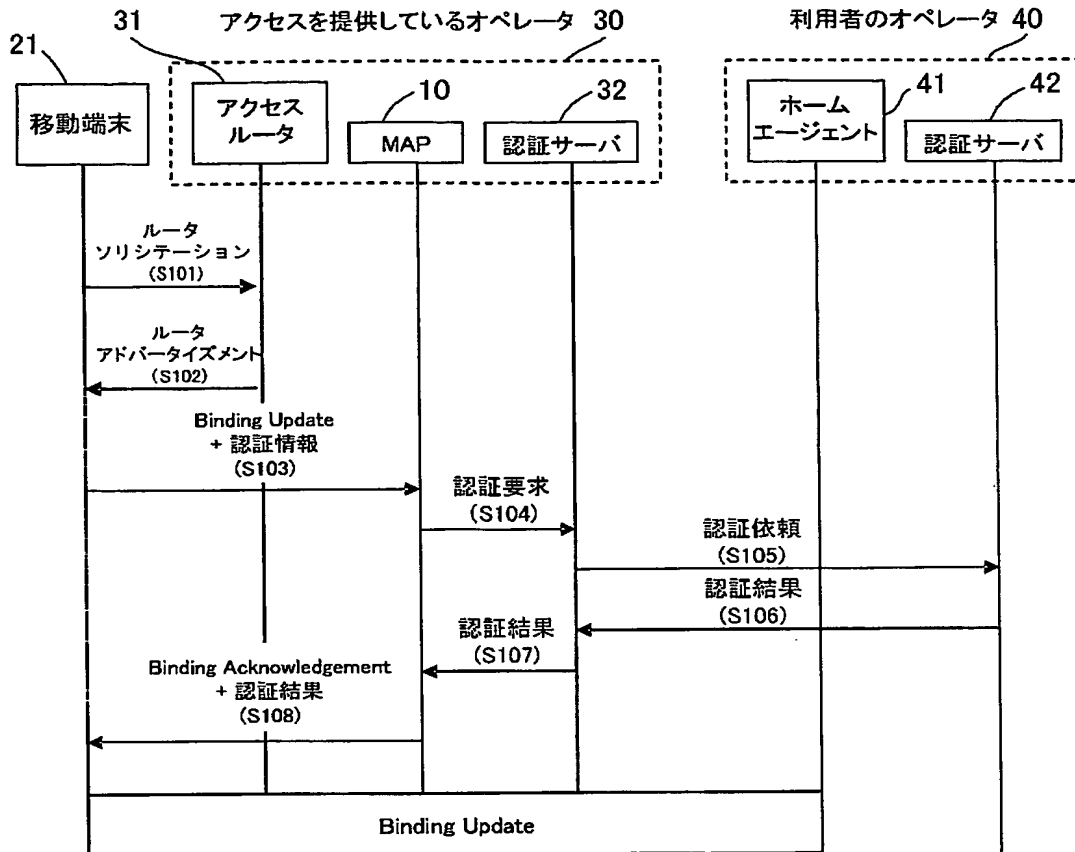
- 10、62 MAP
- 11 上位ネットワーク通信手段
- 12 下位ネットワーク通信手段
- 13 HMIPv6経路制御手段
- 14 認証要求送受信手段
- 15 情報格納手段
- 16 HMIPv6テーブル
- 17 認証サーバのアドレス
- 18 時間管理手段
- 19 状態テーブル
- 20 上位ネットワーク
- 21、51、61 移動端末
- 25 下位ネットワーク
- 30、57、64 アクセスを提供しているオペレータ
- 31 アクセスルータ
- 32、42、53、56 認証サーバ
- 40、58、65 利用者のオペレータ
- 41、55、63 ホームエージェント
- 52 フォーリンエージェント

【書類名】 図面

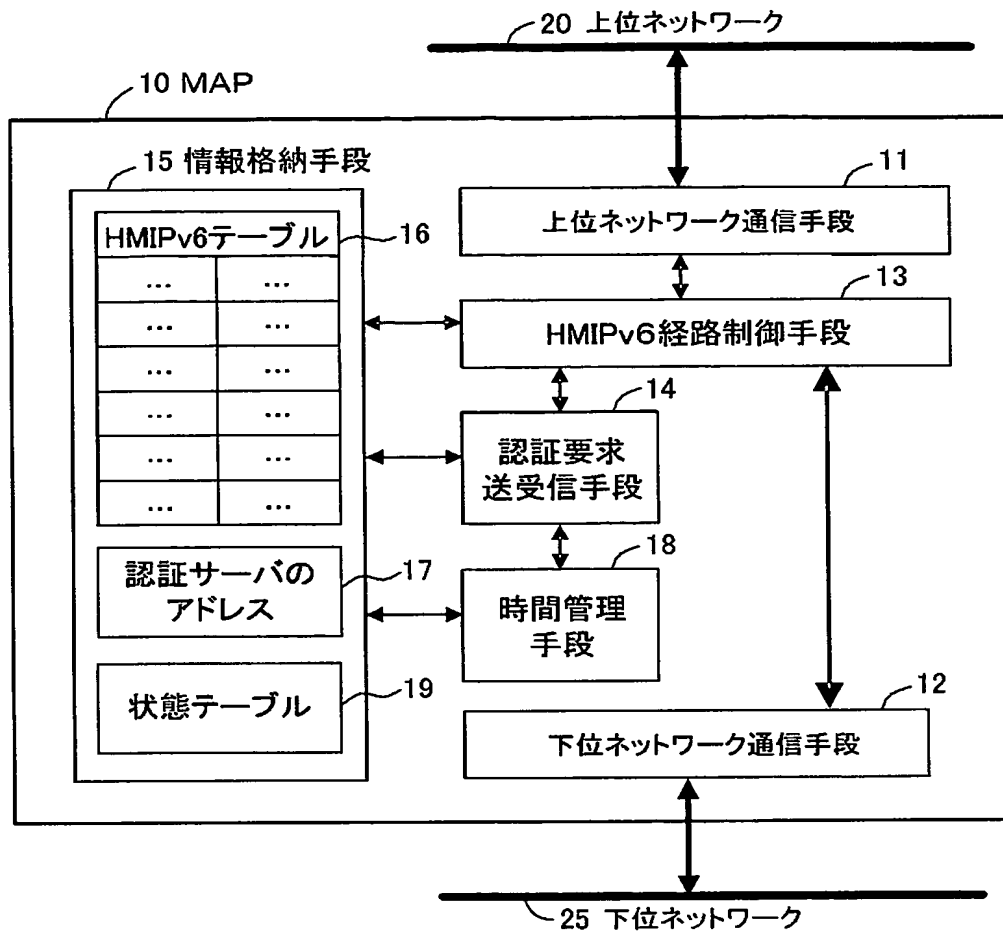
【図 1】



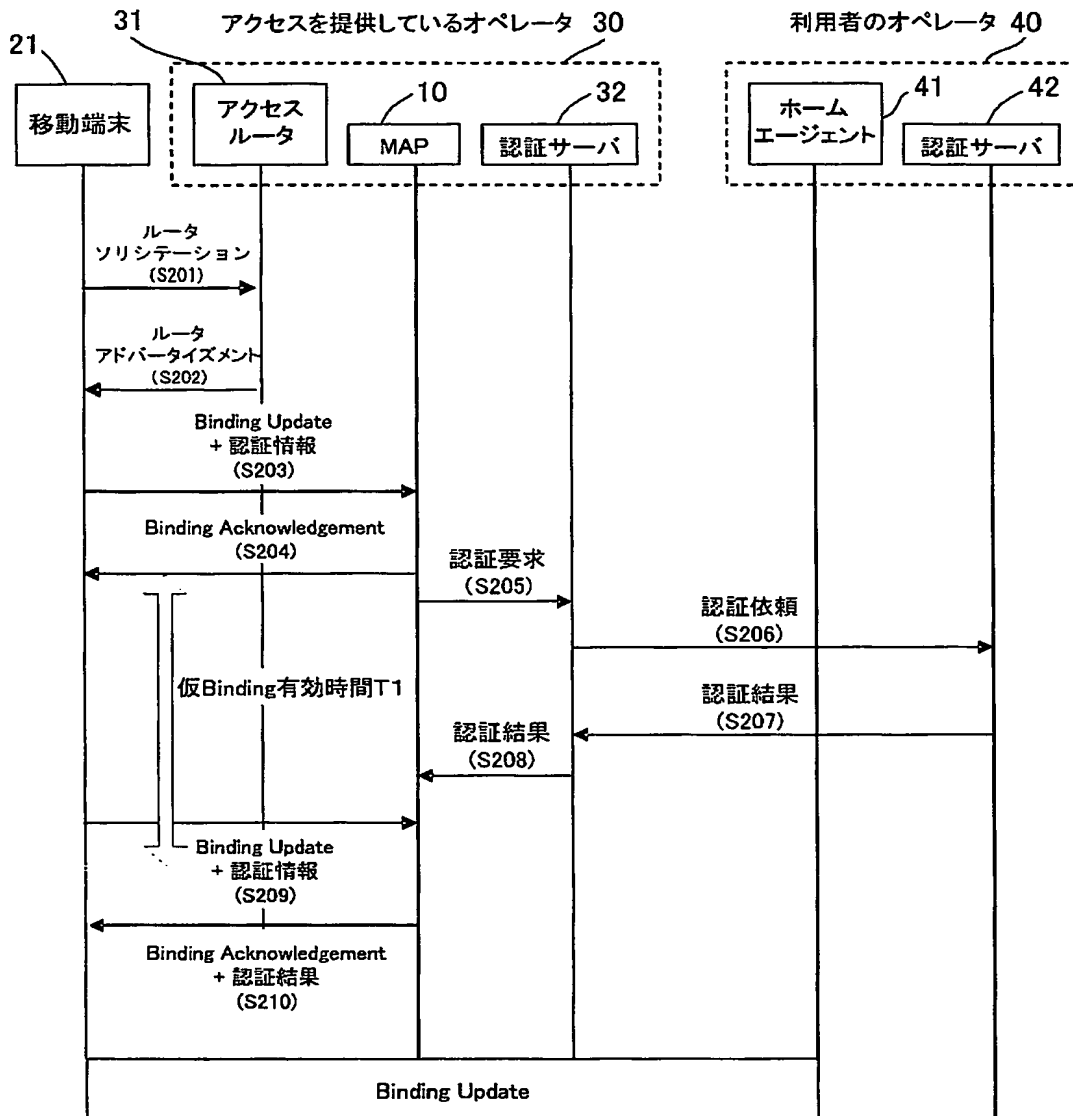
【図 2】



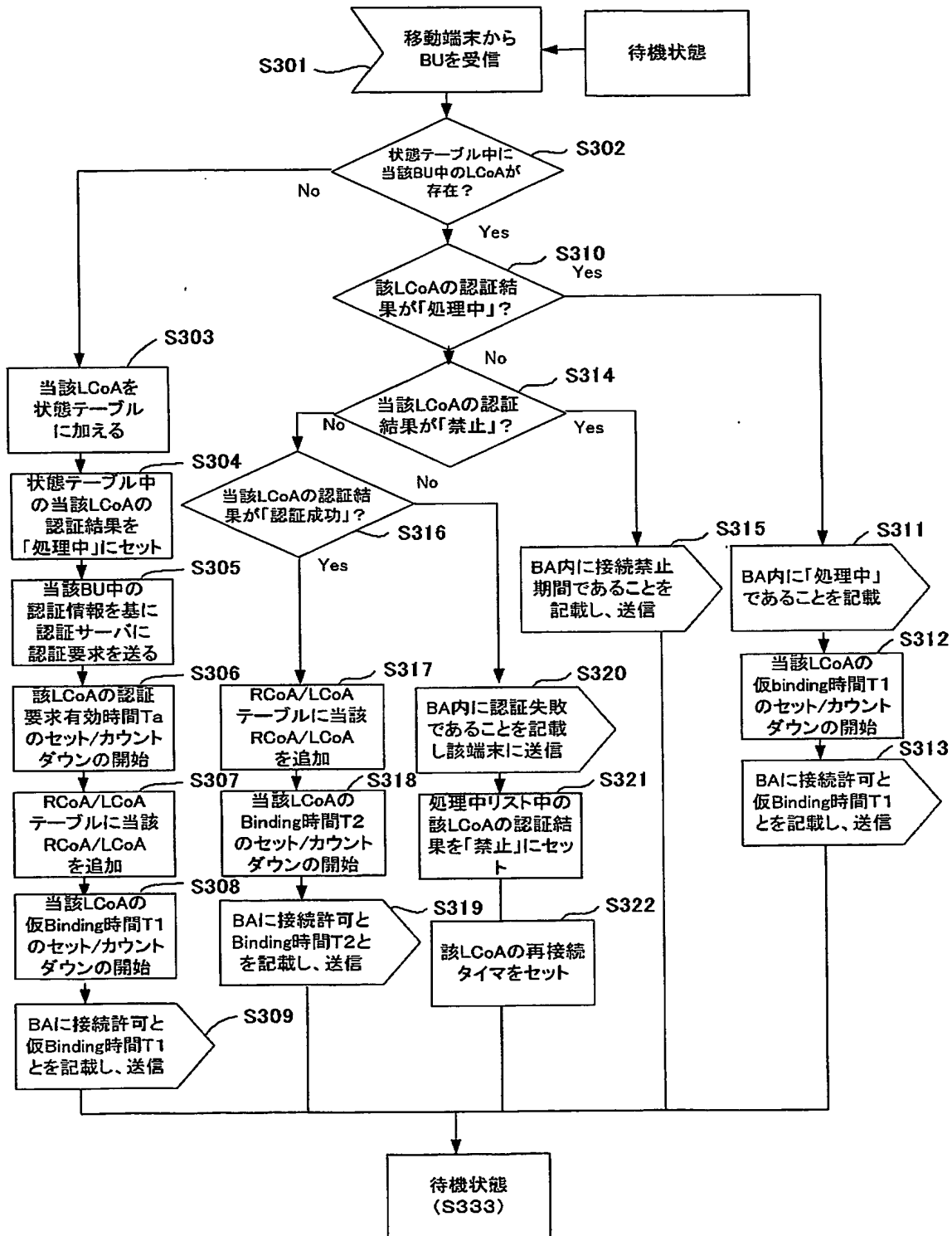
【図 3】



【図 4】



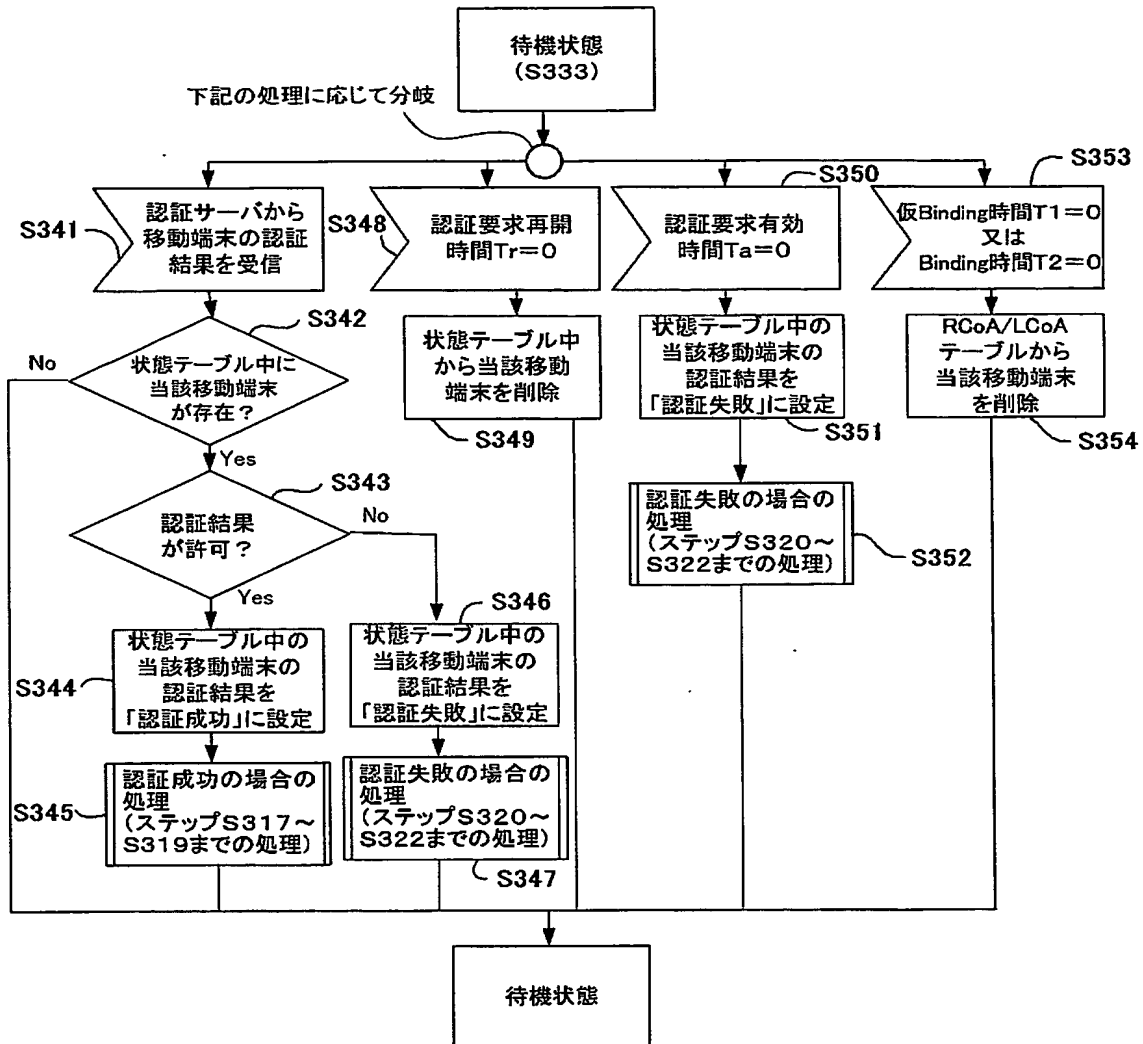
【図 5】



【図 6】

端末の L C o A	認証結果	認証要求有効時間 T a	認証要求再開時間 T r	仮 Binding 時間 T 1 Binding 時間 T 2
2002::ID101	処理中	87	-	45
2002::ID11	認証失敗	-	1532	-
2002::ID334	認証成功	-	-	231003
...

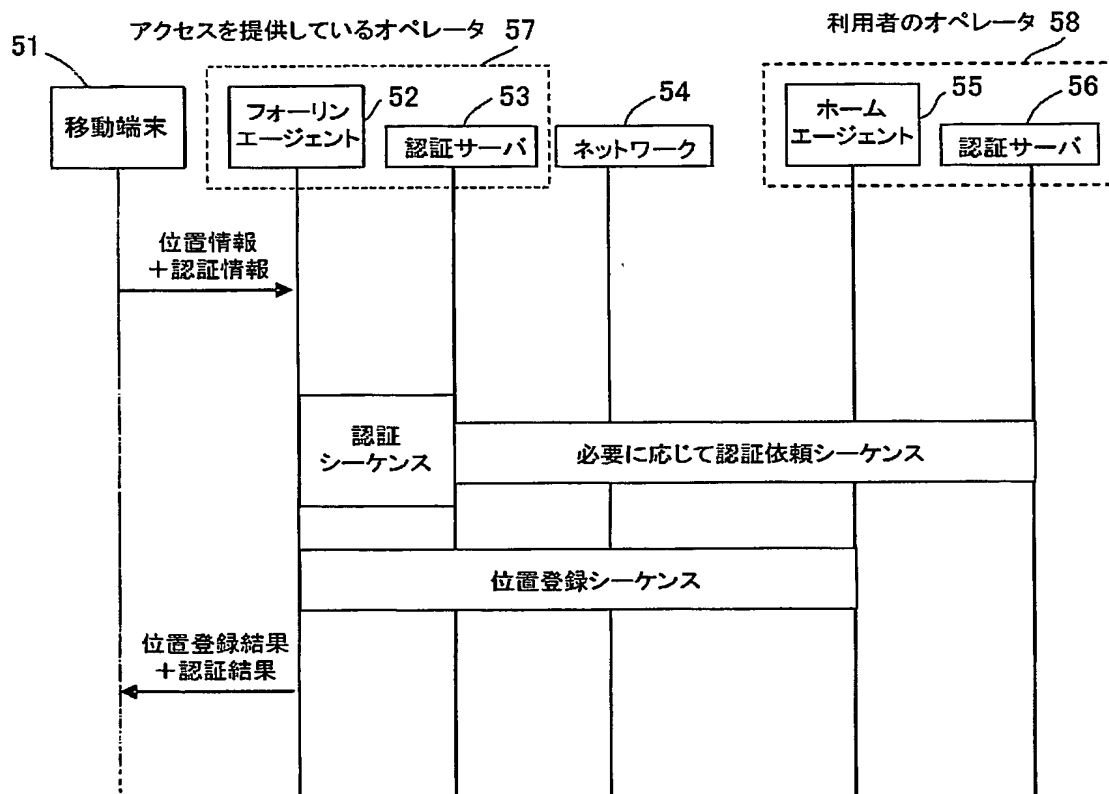
【図 7】



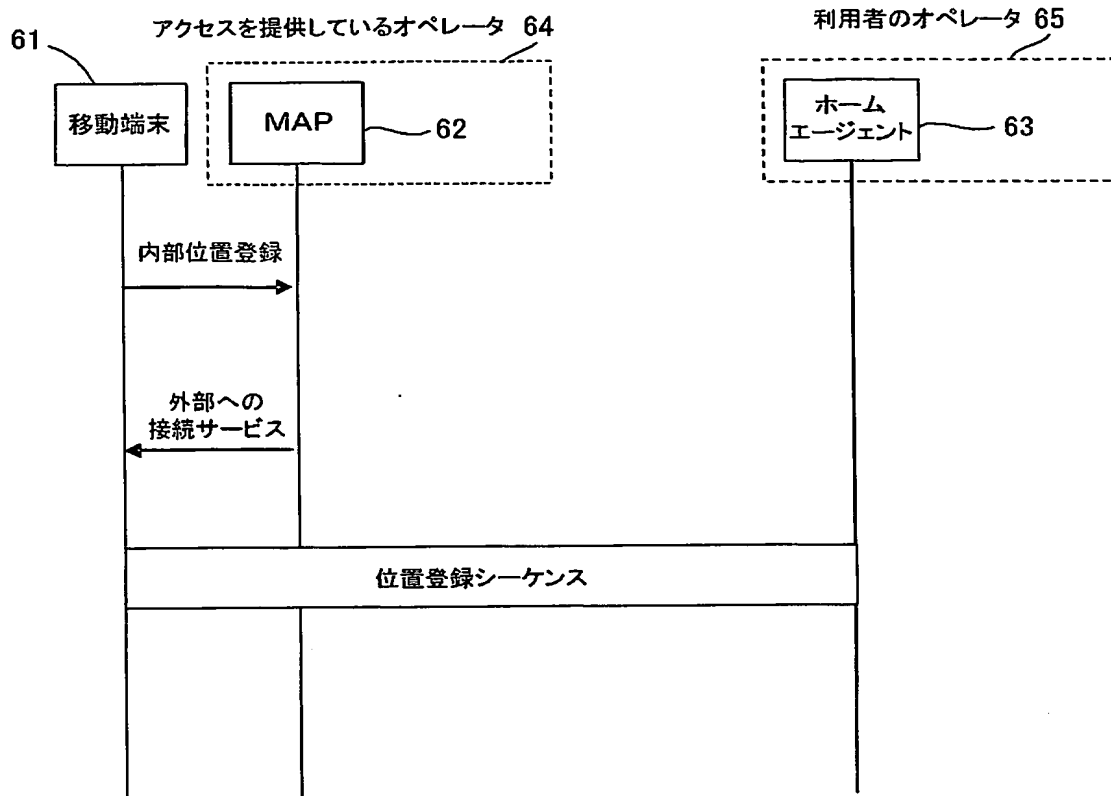
【図 8】

端末ID	認証結果	認証要求有効時間 T _a	認証要求再開時間 T _r	仮 Binding 時間 T ₁ Binding 時間 T ₂
MT101	処理中	87	-	45
MT11	認証失敗	-	1532	-
MT334	認証成功	-	-	231003
...

【図 9】



【図 10】



【書類名】 要約書

【要約】

【課題】 移動端末がリンク接続を変更する際に、スムーズにハンドオーバーを行えるようにするとともに、リンク接続の変更に要する時間を短縮する。

【解決手段】 HMI P v 6 を利用して、移動端末 2 1 が接続リンクの変更を行う際、移動端末のリンク接続を管理するサーバ (MA P 1 0) に対して、リンク接続を変更するための情報 (Binding Update) と同時に、認証情報の送信を行う。MA P は、認証サーバ 3 2 に対して認証要求を行って認証結果を取得した場合、リンク接続の変更の確認情報 (Binding Acknowledgement) と同時に、認証結果の送信を行う。また、MA P は、移動端末から Binding Update と認証情報を受信した後、先に Binding Acknowledgement と仮の接続許可を送り、その後、認証結果を取得して、正式な接続許可を与えるか否かを決定することも可能である。

【選択図】 図 2

認定・付加情報

特許出願の番号	特願 2 0 0 2 - 3 1 1 9 1 0
受付番号	5 0 2 0 1 6 1 5 1 9 5
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 1 4 年 1 0 月 2 8 日

< 認定情報・付加情報 >

【提出日】	平成14年10月25日
-------	-------------

次頁無

特願 2 0 0 2 - 3 1 1 9 1 0

出 願 人 履 歷 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社